

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-256191  
 (43)Date of publication of application : 21.09.2001

(51)Int.Cl. G06F 15/00  
 G06T 7/00

(21)Application number : 2000-064634 (71)Applicant : MITSUBISHI ELECTRIC CORP

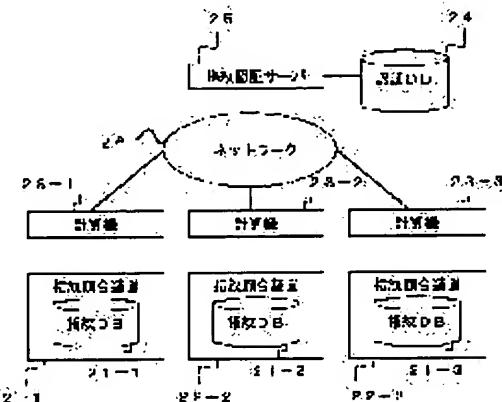
(22)Date of filing : 09.03.2000 (72)Inventor : SADAKANE TETSUO  
 BABA YOSHIMASA  
 OKAZAKI NAONOBU  
 NAKAMURA HIROSHI  
 FUJII TERUKO

## (54) NETWORK FINGERPRINT AUTHENTICATION SYSTEM

### (57)Abstract:

PROBLEM TO BE SOLVED: To reduce the loads of a network and an authentication server while unitarily managing authentication information.

SOLUTION: This system is provided with a fingerprint DB capable of preserving a user identifier and fingerprint information, a fingerprint collation device for collating an inputted user identifier and sampled fingerprint information with the fingerprint DB and outputting the sampled fingerprint information in the case that the collated result matches or in the case that the inputted user identifier is not preserved in the fingerprint DB, a computer for transmitting the authentication information including the fingerprint information outputted from the fingerprint collation device and the user identifier and requesting authentication, an authentication DB for preserving the authentication information including the user identifier and the fingerprint information registered beforehand and a fingerprint authentication server for collating the authentication information transmitted from the computer with the authentication DB and authenticating a fingerprint.



## LEGAL STATUS

[Date of request for examination] 18.03.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-256191

(P2001-256191A)

(43)公開日 平成13年9月21日 (2001.9.21)

(51)Int.Cl.<sup>7</sup>  
G 0 6 F 15/00  
G 0 6 T 7/00

識別記号  
3 3 0

F I  
G 0 6 F 15/00  
15/62

テ-マコ-ト<sup>8</sup> (参考)  
3 3 0 F 5 B 0 4 3  
4 6 0 5 B 0 8 5

審査請求 未請求 請求項の数11 O L (全 15 頁)

(21)出願番号 特願2000-64634(P2000-64634)  
(22)出願日 平成12年3月9日 (2000.3.9)

(71)出願人 000006013  
三菱電機株式会社  
東京都千代田区丸の内二丁目2番3号  
(72)発明者 貞包 哲男  
東京都千代田区丸の内二丁目2番3号 三菱  
電機株式会社内  
(72)発明者 馬場 義昌  
東京都千代田区丸の内二丁目2番3号 三菱  
電機株式会社内  
(74)代理人 100102439  
弁理士 宮田 金雄 (外1名)

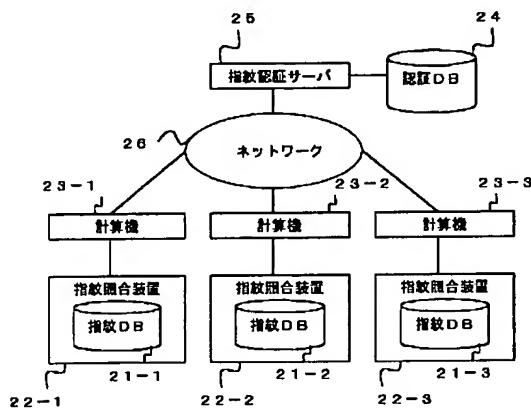
最終頁に続く

(54)【発明の名称】 ネットワーク指紋認証システム

(57)【要約】

【課題】 認証情報の一元管理を行いながら、ネットワークと認証サーバの負荷軽減を実現する。

【解決手段】 使用者識別子と指紋情報とが保存可能な指紋DBと、入力された使用者識別子と採取した指紋情報とを前記指紋DBと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DBに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証DBと、前記計算機から送信された認証情報と前記認証DBと照合して指紋認証を行う指紋認証サーバとを備える。



## 【特許請求の範囲】

【請求項1】 使用者識別子と指紋情報とが保存可能な指紋DBと、

入力された使用者識別子と採取した指紋情報を前記指紋DBと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DBに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、

前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、

予め登録された使用者識別子と指紋情報を含む認証情報が保存された認証DBと、

前記計算機から送信された認証情報と前記認証DBと照合して指紋認証を行う指紋認証サーバとを備えたことを特徴とするネットワーク指紋認証システム。

【請求項2】 前記指紋照合装置は、前記指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋DBに保存されていない場合に、前記入力された使用者識別子と採取した指紋情報を前記指紋DBに保存するように構成されたことを特徴とする請求項1に記載のネットワーク指紋認証システム。

【請求項3】 前記指紋照合装置での指紋照合のしきい値が、指紋認証サーバでの指紋照合のしきい値より低く設定されたことを特徴とする請求項1又は請求項2に記載のネットワーク指紋認証システム。

【請求項4】 前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証成功である度に、当該採取した指紋情報を前記指紋DBに保存するように構成されたことを特徴とする請求項1ないし請求項3のいずれかに記載のネットワーク指紋認証システム。

【請求項5】 前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証失敗であった場合に当該採取した指紋情報と入力された使用者識別子とを前記指紋DBに保存し、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報を後に採取した指紋情報を照合し、一致する場合には当該後に採取した指紋情報を前記計算機に出力しないように構成されたことを特徴とする請求項1ないし請求項4のいずれかに記載のネットワーク指紋認証システム。

【請求項6】 前記計算機は、前記採取した指紋情報と前記指紋DBに保存された指紋情報との照合度を使用者に提示可能に構成されたことを特徴とする請求項1ないし請求項5のいずれかに記載のネットワーク指紋認証システム。

【請求項7】 前記指紋照合装置は、前記指紋認証サーバに登録されている指紋情報が変更された場合に、前記

指紋DBに保存されている指紋情報を削除するように構成されたことを特徴とする請求項1ないし請求項6のいずれかに記載のネットワーク指紋認証システム。

【請求項8】 前記指紋照合装置は、前記指紋DBに保存された指紋情報を所定時間後に削除するように構成されたことを特徴とする請求項1ないし請求項7のいずれかに記載のネットワーク指紋認証システム。

【請求項9】 採取した指紋情報を出力する指紋照合装置と、

前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、

使用者識別子と指紋情報を保存可能な指紋DBと、前記計算機から送信された認証情報に含まれた指紋情報とその使用者識別子とを前記指紋DBと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DBに保存されていない場合に、前記認証情報を出力する指紋認証キャッシュ・サーバと、

予め登録された使用者識別子と指紋情報を含む認証情報が保存された認証DBと、

前記指紋認証キャッシュ・サーバから出力された認証情報と上記認証DBと照合して指紋認証を行う指紋認証サーバとを備えたことを特徴とするネットワーク指紋認証システム。

【請求項10】 前記指紋認証キャッシュ・サーバは、照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたことを特徴とする請求項9に記載のネットワーク指紋認証システム。

【請求項11】 前記計算機は、前記指紋認証結果に基づいてアプリケーションの制御を行うように構成されたことを特徴とする請求項1ないし請求項10のいずれかに記載のネットワーク指紋認証システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、採取した指紋情報を用いて指紋認証を行うネットワーク指紋認証システムに関するものである。

## 【0002】

【従来の技術】図9は例えば、特開平8-329010号公報に示された従来のネットワーク認証システムであり、認証処理を行う複数のコンピュータシステムが通信網を介して相互に接続されたコンピュータネットワークシステムにおいて、該当コンピュータシステムに認証処理のための情報がない場合のみ、ネットワークを介して他のコンピュータシステムに認証処理を依頼することにより、ネットワーク上のデータ通信効率を向上を可能にしたものである。

【0003】図9の説明を行う。図9に示されるコンピュータネットワークシステムは、アクセス権の有無を判定するための照合処理を行う複数のコンピュータシステ

証情報を送信して認証依頼する計算機と、予め登録された使用者識別子と指紋情報を含む認証情報を保存された認証DBと、前記計算機から送信された認証情報と前記認証DBと照合して指紋認証を行う指紋認証サーバとを備えたものである。

【0015】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋DBに保存されていない場合に、前記入力された使用者識別子と採取した指紋情報をと前記指紋DBに保存するように構成されたものである。

【0016】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置での指紋照合のしきい値が、指紋認証サーバでの指紋照合のしきい値より低く設定されたものである。

【0017】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証成功である度に、当該採取した指紋情報を前記指紋DBに保存するように構成されたものである。

【0018】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証失敗であった場合に当該採取した指紋情報をと入力された使用者識別子とを前記指紋DBに保存し、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報を後に採取した指紋情報を照合し、一致する場合には当該後に採取した指紋情報を前記計算機に出力しないように構成されたものである。

【0019】また、つぎの発明に係るネットワーク指紋認証システムは、前記計算機は、前記採取した指紋情報と前記指紋DBに保存された指紋情報との照合度を使用者に提示可能に構成されたものである。

【0020】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記指紋認証サーバに登録されている指紋情報が変更された場合に、前記指紋DBに保存されている指紋情報を削除するように構成されたものである。

【0021】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記指紋DBに保存された指紋情報を所定時間後に削除するように構成されたものである。

【0022】さらにまた、つぎの発明に係るネットワーク指紋認証システムは、採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報をとその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、使用者識別子と指紋情報をと保存可能な指紋DBと、前記計算機から送信された認証情報を

含まれた指紋情報とその使用者識別子とを前記指紋DBと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DBに保存されていない場合に、前記認証情報を出力する指紋認証キャッシュ・サーバと、予め登録された使用者識別子と指紋情報をと含む認証情報を保存された認証DBと、前記指紋認証キャッシュ・サーバから出力された認証情報をと上記認証DBと照合して指紋認証を行う指紋認証サーバとを備えたものである。

【0023】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋認証キャッシュ・サーバは、照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたものである。

【0024】また、つぎの発明に係るネットワーク指紋認証システムは、前記計算機は、前記指紋認証結果に基づいてアプリケーションの制御を行うように構成されたものである。

【0025】  
【発明の実施の形態】実施の形態1. 図1はこの発明の実施の形態1の全体的な構成を示すシステム構成図である。図において、21-1～3は、使用者識別子と指紋情報をと保存可能な指紋DBであり、ここでは指紋照合装置の内部に設置されている。また、予め使用者識別子と指紋情報をと保存されている。22-1～3は、使用者の指紋情報を採取すると共に、入力された使用者識別子と採取した指紋情報をと前記指紋DB21-1～3と照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DB21-1～3に保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置である。また、ここでは、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋DB21-1～3に保存されていない場合に、前記入力された使用者識別子と採取した指紋情報をと前記指紋DB21-1～3に保存するように構成されている。

【0026】23-1～3は、前記指紋照合装置22-1～3から出力された指紋情報をとその使用者識別子とを含む認証情報を指紋認証サーバに送信して認証依頼する計算機であり、ここでは、指紋取得のための使用者への指示を行うと共に、使用者識別子を前記指紋照合装置22-1～3に入力し、指紋認証サーバの指紋認証結果に基づいてアプリケーションの制御を行うように構成されている。

【0027】24は、予め登録された使用者識別子と指紋情報をと含む認証情報を保存された認証DBである。ここでは、認証の対象となる使用者の使用者識別子や指紋情報を前記アプリケーションに対するアクセス制御情報等を管理するように構成されている。25は、前記計算機23-1～3から送信された認証情報をと前記認証DB24と照合し、その指紋認証結果を前記計算機23-

1～3に送信する指紋認証サーバである。26は、前記指紋認証サーバ25と複数の計算機23-1～3とを接続するネットワークである。

【0028】次に動作について図2を用いて説明する。まず、指紋照合装置22は、計算機23の指示により使用者から指紋情報の採取を行う(ステップS31)。この時に、指紋情報を採取する使用者の使用者識別子も計算機23より受取る。そして、上記の使用者識別子を用いて指紋DB21にアクセスして該当使用者の指紋情報が保存されているかを判断する(ステップS32)。指紋情報が保存されていない場合は、計算機23にその採取した指紋情報を送信する(ステップS34)。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する(ステップS33)。ステップS33で、指紋照合が一致した場合には、採取した指紋情報を計算機23に送信する(ステップS34)。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う(ステップS31)。

【0029】次に、計算機23は、受信した指紋情報を使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS35)。

【0030】次に、指紋認証サーバ25は、受信した認証情報を認証DB24に保存されている認証情報を用いて認証を行う(ステップS36)。認証成功の場合には、認証成功のレスポンスを計算機23に送信する。認証失敗の場合には認証失敗のレスポンスを計算機23に送信する。

【0031】次に、計算機23は、指紋認証サーバ25のレスポンスが認証成功の場合、アプリケーションの実行をする(ステップS37)。認証失敗の場合、ユーザに通知して終了する。

【0032】次に、計算機23でアプリケーションが実行された場合(ステップS37)、指紋照合装置22は、指紋DB21に該当指紋情報が保存されているかを判断する(ステップS38)。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報を使用者識別子を指紋DB21に保存する(ステップS39)。

【0033】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋照合装置で指紋照合を行い、その指紋照合結果が一致した場合、又は、入力された使用者識別子が指紋DBに保存されていない場合に、指紋認証サーバで指紋認証を行うようにしたことにより、指紋認証サーバへの送信回数を軽減でき、使用者の利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、認証DBで認証情報を一元管理することにより、管理コスト、認証情報の秘匿のセキュリティの向上が可能となる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側(本実施の形態では計算機、指紋照合装置、

指紋DB)だけの変更で適用可能である。また、最終的には指紋認証サーバが指紋認証の判断を行うので、認証精度の整合性を保つことができる。

【0034】また、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋DBに保存されていない場合に、入力された使用者識別子と採取した指紋情報を前記指紋DBに保存するようにしたことにより、次回以降の指紋照合において、当該使用者の指紋照合を指紋照合装置で行うことができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側だけの変更で適用可能である。

【0035】また、計算機は、指紋認証サーバでの指紋認証結果に基づいてアプリケーションの制御を行うようにしたことにより、使用者に指紋認証結果に応じたアプリケーションを提供することができる。

【0036】実施の形態2. 以上の実施の形態1では、指紋認証サーバで指紋照合する前に、指紋照合装置で指紋照合を行い、指紋認証サーバでの指紋認証を成功しやすくするようにしたものである。通常、指紋照合では、所定のしきい値以上の照合度があった場合に、2つの指紋が一致するように判定する。次に、指紋認証サーバの指紋照合では一致するが、指紋照合装置の指紋照合では一致しないような指紋情報を対応できるように、指紋照合装置での指紋照合で一致するように、指紋照合装置での照合のしきい値を低くした実施の形態を示す。

【0037】実施の形態1と同様に図1は、この発明の実施の形態2の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋照合装置22での指紋照合のしきい値(照合度のしきい値)が、指紋認証サーバ25の照合度のしきい値より低く設定されている。すなわち、指紋認証サーバ25のしきい値は、各指紋照合装置22-1～3を一元管理するために設定されたしきい値であるのに対し、各指紋照合装置22-1～3のしきい値は、前記指紋認証サーバ25のしきい値より低くなるように、それぞれ個別に設定されたものである。

【0038】次に、動作について図2を用いて説明する。まず、指紋照合装置22は、計算機23の指示により使用者から指紋情報の採取を行う(ステップS31)。この時に、指紋情報を採取する使用者の使用者識別子も計算機23より受取る。そして、上記の使用者識別子を用いて指紋DB21にアクセスして該当使用者の指紋情報が保存されているかを判断する(ステップS32)。指紋情報が保存されていない場合は、計算機23にその採取した指紋情報を送信する(ステップS34)。指紋情報が保存されている場合には、その保存されている指紋情報を採取した指紋情報を照合する(ステップS33)。ステップS33で、指紋照合が一致した場合には、採取した指紋情報を計算機23に送信する

ム11(11-1~11-3)が通信網12を介して相互に接続されている。各コンピュータシステム11にはそれぞれデータ縮退ユニット13(13-1~13-3)を介し、使用者の身体的特徴(特徴データ)を計測する特徴計測ユニット14(14-1~14-3)がそれぞれ接続されている。このデータ縮退ユニット14により使用者の身体的特徴が電気信号として抽出される。各コンピュータシステム11には、それぞれファイルシステム15(15-1~15-3)が接続されている。このファイルシステム15は、アクセス権の有無を判定するための照合処理の際に参照される登録特徴データ、及び処理対象となる各種ファイル・データが格納されている。尚、接続されるコンピュータシステムの数はこれに限定されない。

【0004】次に動作について説明する。図10及び図11に示されるフローチャートを参照して、図9に示されるコンピュータネットワークシステムのファイルアクセス動作について述べる。

【0005】図9に示されるコンピュータネットワークシステムにおいて、任意のコンピュータシステム11でファイルのアクセス要求が発生すると、このコンピュータ11では、特徴計測ユニット14を用いて身体的特徴、例えば指の指紋等を入力するよう要求する。ここで、使用者の指紋が特徴計測ユニット14に置かれたと、データ縮退ユニット13により縮退された特徴データが抽出する(ステップS11、S12)。

【0006】抽出された特徴データ(抽出特徴データ)は、アクセス要求の発生した日時や、パスワード等の使用者識別子に付加される(ステップS13)。尚、日時やパスワード等の使用者識別子を付与せず、縮退された抽出特徴データのみを用いてもよい。

【0007】次に、コンピュータシステム11では、アクセス要求されたファイルがこのコンピュータシステム11に接続されているファイルシステム15に格納されているか否かを判定する(ステップS14)。ここで、ファイルシステム15にアクセス要求されたファイルが格納されている場合、ファイルシステム15に格納されている登録特徴データと、前記抽出特徴データ及び使用者識別子が同一であるか調べるために照合処理を行う(ステップS16)。一致する場合は、ファイルにアクセスし(ステップS17)、一致しない場合は、ファイルアクセスが不可能である通知等を行った後、ファイルアクセス要求に応じた処理が終了する。

【0008】前記ステップS14において、ファイルシステム15にアクセス要求されたファイルが格納されていない場合、コンピュータシステム11は、アクセス要求するファイルのファイル名と共に前記抽出特徴データ及び使用者識別子を、通信網12を介して他のコンピュータシステムに送信する(ステップS18)。この後、抽出特徴データ等を送出した送り先のコンピュータシス

テムからの応答を受信し、アクセスの可否に応じて前述したような処理を行う(ステップS19)。尚、後述するがアクセス可の場合、アクセス要求したファイルが送られるので、これをファイルシステム15に格納する。【0009】次に、前記ステップS18において送出された各種データを受信したコンピュータシステム11の処理を図11を参照して説明する。

【0010】コンピュータシステム11は、他のコンピュータシステムからアクセス要求のあったファイルのファイル名等と共に前記抽出特徴データ及び使用者識別子を受信すると(ステップS21)、アクセス要求されているファイルが自コンピュータシステム11に接続されているファイルシステム15に接続されたファイルシステム15に格納されているか否か判定する(ステップS22)。ここで、ファイルシステム15に要求されたファイルが格納されていない場合、この旨を要求元のコンピュータシステムに通知する(ステップS23)。

【0011】前記ステップS22において、アクセス要求されたファイルがファイルシステム15に格納されている場合、ステップS21において受信した抽出特徴データ及び使用者識別子を用い、要求元の使用者にファイルアクセス権が有るか否かを決定するための照合処理を行う(ステップS24、S25)。照合結果が一致である場合は、アクセス要求されたファイルを送信し(ステップS26)、照合結果が不一致である場合は、ファイルのアクセス権が無いことを要求元のコンピュータシステムに通知する(ステップS27)。

【0012】

【発明が解決しようとする課題】以上のように、従来のネットワーク指紋認証システムにおいては、ネットワークの負荷軽減、認証サーバの負荷分散を実現するため、認証処理を行う複数のコンピュータシステムをネットワークを介して相互に接続し、認証に必要な情報(認証情報)を分散管理していたため、認証情報の登録・削除・変更等の管理時に整合性を保つのが困難であり、場合によってはかえってネットワーク、認証サーバに負荷がかかってしまうという問題点があった。

【0013】この発明は上記のような問題点を解決するためになされたもので、認証情報の一元管理を行いながら、ネットワークと認証サーバの負荷軽減を実現することを目的とする。

【0014】

【課題を解決するための手段】この発明に係るネットワーク指紋認証システムは、使用者識別子と指紋情報とが保存可能な指紋DBと、入力された使用者識別子と採取した指紋情報を前記指紋DBと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DBに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認

(ステップS34)。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う(ステップS31)。尚、前述のステップS33での指紋照合に用いるしきい値は、後述する指紋認証サーバでの指紋照合に用いるしきい値より低く設定されている。

【0039】次に、計算機23は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS35)。

【0040】次に、指紋認証サーバ25は、受信した認証情報と認証DB24に保存されている認証情報を用いて認証を行う(ステップS36)。認証成功の場合には、認証成功的レスポンスを計算機23に送信する。認証失敗の場合には認証失敗のレスポンスを計算機23に送信する。尚、前述のステップS36の認証で行われる指紋照合に使用されるしきい値は、複数の指紋照合装置22-1~3を一元管理するために設定されたしきい値(通常のしきい値)であり、指紋照合装置に設定されたしきい値より高く設定されたしきい値を使用する。

【0041】次に、計算機23は、指紋認証サーバ25のレスポンスが認証成功の場合、アプリケーションの実行をする(ステップS37)。認証失敗の場合、ユーザに通知して終了する。

【0042】次に、計算機23でアプリケーションが実行された場合(ステップS37)、指紋照合装置22は、指紋DB21に該当指紋情報が保存されているかを判断する(ステップS38)。保存されている場合は、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋DB21に保存する(ステップS39)。

【0043】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋照合装置での指紋照合のしきい値を、指紋認証サーバでの指紋照合のしきい値より低く設定したことにより、指紋照合認証サーバでの指紋照合で一致するはずの指紋情報が、指紋照合装置での指紋照合で失敗する可能性が低くなるので、使用者の指紋の採取の回数が少なくなり、使用者の利便性の向上が実現できる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側(本実施の形態では指紋照合装置)だけの変更で適用可能である。

【0044】実施の形態3. 以上の実施の形態2では、指紋照合装置での指紋照合は一致しないが、指紋認証サーバで指紋照合させた場合に一致するような指紋を採取した場合に、指紋照合装置での照合で一致するように、指紋照合装置での照合のしきい値を低くしたものであったが、次に、指紋認証サーバでの認証が成功した最新の使用者から採取した指紋を、指紋照合装置に保存する実施の形態を示す。

【0045】実施の形態1と同様に図1は、この発明の実施の形態3の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。こ

の実施の形態では、指紋照合装置22は、採取した指紋情報の指紋認証サーバ25での指紋認証結果が認証成功である度に、当該採取した指紋情報を指紋DB21に保存するように構成されている。

【0046】次に、動作について図3用いて説明する。まず、指紋照合装置22は、計算機23の指示により使用者から指紋情報の採取を行う(ステップS41)。この時に、指紋情報を採取する使用者の使用者識別子も計算機23より受取る。そして、上記の使用者識別子を用いて指紋DB21にアクセスして該当使用者の指紋情報が保存されているかを判断する(ステップS42)。指紋情報が保存されていない場合は、計算機23にその採取した指紋情報を送信する(ステップS44)。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する(ステップS43)。ステップS43で、指紋照合が一致した場合には、採取した指紋情報を計算機23に送信する(ステップS44)。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う(ステップS41)。

【0047】次に、計算機23は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS45)。

【0048】次に、指紋認証サーバ25は、受信した認証情報と認証DB24に保存されている認証情報を用いて認証を行う(ステップS46)。認証成功の場合には、認証成功的レスポンスを計算機23に送信する。認証失敗の場合には認証失敗のレスポンスを計算機23に送信する。

【0049】次に、計算機23は、指紋認証サーバ25のレスポンスが認証成功の場合、アプリケーションの実行をする(ステップS47)。認証失敗の場合、ユーザに通知して終了する。

【0050】次に、計算機23でアプリケーションが実行された場合(ステップS47)、指紋照合装置22は、採取した指紋情報と使用者識別子を指紋DB21に保存する(ステップS48)。

【0051】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋認証サーバでの指紋認証が成功した最新の指紋情報を指紋DBに保存することにより、指紋照合装置での照合で失敗する可能性が低くなるので、使用者の指紋の採取の回数が少なくなり、使用者の利便性の向上が実現できる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側(本実施の形態では計算機、指紋照合装置、指紋DB)だけの変更で適用可能である。

【0052】実施の形態4. 以上の実施の形態3は、指紋認証サーバでの認証が成功した最新の使用者から採取した指紋を、指紋照合装置に保存するものであったが、次に指紋認証サーバでの認証が失敗であった場合の指紋も保存し、次に指紋を採取した場合に、その失敗した指

紋と照合した結果が一致した場合には、再度指紋を採取し直す実施の形態を示す。

【0053】実施の形態1と同様に図1は、この発明の実施の形態4の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋照合装置22は、採取した指紋情報の指紋認証サーバ25での指紋認証結果が認証失敗であった場合に当該採取した指紋情報と入力された使用者識別子とを指紋DB21に保存しておき、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報と後に採取した指紋情報を照合し、一致する場合には当該後に採取した指紋情報を計算機23に出力しないように構成されている。また、前記認証失敗であった指紋情報と後に採取した指紋情報を照合する指紋照合のしきい値は、指紋認証サーバ25で使用されるしきい値より高く設定されている。

【0054】次に、動作について図4を用いて説明する。まず、指紋照合装置22は、計算機23の指示により使用者から指紋情報の採取を行う(ステップS51)。この時に、指紋情報を採取する使用者の使用者識別子も計算機23より受取る。そして、上記の使用者識別子を用いて指紋DB21にアクセスして該当使用者の指紋情報が保存されているかを判断する(ステップS52)。指紋情報が保存されていない場合は、計算機23にその採取した指紋情報を送信する(ステップS54)。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する(ステップS53)。ステップS53で、指紋認証サーバ25の指紋認証で認証成功となった指紋情報との指紋照合が一致した場合には、採取した指紋情報を計算機23に送信する(ステップS54)。指紋認証サーバ25の指紋認証で認証成功となった指紋情報との指紋照合が一致しない場合、又は、指紋認証サーバ25の指紋認証で認証失敗となった指紋情報との指紋照合が一致した場合には、もう一度指紋情報の採取を行う(ステップS51)。尚、ステップS53で、認証失敗の指紋情報との指紋照合に用いるしきい値は、指紋認証サーバ25での指紋照合に用いるしきい値より高く設定されている。

【0055】次に、計算機23は、受信した指紋情報を使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS55)。

【0056】次に、指紋認証サーバ25は、受信した認証情報を認証DB24に保存されている認証情報を用いて認証を行う(ステップS56)。認証成功の場合には、認証成功的レスポンスを計算機23に送信する。認証失敗の場合には認証失敗のレスポンスを計算機23に送信する。尚、前述のステップS56の認証で行われる指紋照合に用いるしきい値は、複数の指紋照合装置22-1~3を一元管理するために設定されたしきい値

(通常のしきい値)である。

【0057】次に、計算機23は、指紋認証サーバ25のレスポンスが認証成功の場合、アプリケーションの実行をする(ステップS57)。

【0058】次に、指紋照合装置において計算機でアプリケーションが実行された(ステップS57)場合、指紋DB22に該当指紋情報が保存されているかを判断する(ステップS58)。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と

10 使用者識別子と認証結果を指紋DB22に保存する(ステップS59)。また、ステップS56で認証失敗の場合には、採取した指紋情報と使用者識別子と認証結果を指紋DB22に保存し(ステップS59)、終了する。

【0059】以上のように、この実施の形態のネットワーク指紋認証システムによれば、一度指紋認証サーバで認証失敗になった指紋情報と一致する指紋情報を指紋認証サーバに送らないようにすることにより、以前認証失敗となった指紋情報と同じような指紋情報は指紋認証サーバへ送信されないので、指紋認証サーバへの送信回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側(本実施の形態では計算機、指紋照合装置、指紋DB)だけの変更で適用可能である。

【0060】また、指紋認証サーバで認証失敗になった指紋情報と後に採取した指紋情報を照合する場合に使用するしきい値を指紋認証サーバで使用するしきい値よりも高く設定したことにより、指紋認証サーバでの指紋照合で一致するはずの指紋情報を、指紋照合装置が指紋認証サーバに送らないようにする可能性を低くすることができます。

【0061】実施の形態5、以上のように実施の形態4は、指紋認証サーバで認証が失敗した指紋を指紋照合装置において利用して、指紋認証サーバに送信しても認証が失敗するとわかっている認証情報を送信しないものであったが、次に、指紋照合装置で照合を行った場合の照合度をユーザに提示する実施の形態を示す。

【0062】実施の形態1と同様に図1は、この発明の実施の形態5の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、計算機23は、採取した指紋情報と指紋DB21に保存された指紋情報との照合度を使用者に提示可能に構成されている。

【0063】次に動作について図2を用いて説明する。まず、指紋照合装置22は、計算機23の指示により使用者から指紋情報の採取を行う(ステップS31)。この時に、指紋情報を採取する使用者の使用者識別子も計算機23より受取る。そして、上記の使用者識別子を用

いて指紋DB21にアクセスして該当使用者の指紋情報を保存されているかを判断する(ステップS32)。指紋情報が保存されていない場合は、計算機23にその採取した指紋情報を送信する(ステップS34)。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する(ステップS33)。この時、指紋照合装置22はその照合度を計算機23に送信し、計算機23はその照合度を使用者に提示する。ステップS33で、指紋照合が一致した場合には、採取した指紋情報を計算機23に送信する(ステップS34)。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う(ステップS31)。

【0064】次に、計算機23は、受信した指紋情報を使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS35)。

【0065】次に、指紋認証サーバ25は、受信した認証情報と認証DB24に保存されている認証情報を用いて認証を行う(ステップS36)。認証成功の場合には、認証成功的レスポンスを計算機23に送信する。認証失敗の場合には認証失敗のレスポンスを計算機23に送信する。

【0066】次に、計算機23は、指紋認証サーバ25のレスポンスが認証成功の場合、アプリケーションの実行をする(ステップS37)。認証失敗の場合、ユーザに通知して終了する。

【0067】次に、計算機23でアプリケーションが実行された場合(ステップS37)、指紋照合装置22は、指紋DB21に該当指紋情報が保存されているかを判断する(ステップS38)。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋DB21に保存する(ステップS39)。

【0068】以上のように、この実施の形態のネットワーク指紋認証システムによれば、採取した指紋情報と指紋DBに保存された指紋情報との指紋照合の照合度を使用者に提示することにより、当該使用者が指の置き方を学習するので、採取される指紋情報が安定し、サーバへの送信回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側(本実施の形態では計算機、指紋照合装置)だけの変更で適用可能である。

【0069】実施の形態6. 以上のように、実施の形態5は、指紋照合装置の中で照合する場合に照合度を使用者に提示するものであったが、次に、認証DBに保存されている指紋情報を変更した場合に対応できる実施の形態を示す。

【0070】実施の形態1と同様に図1は、この発明の実施の形態2の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。こ

の実施の形態では、指紋認証サーバ25は、認証DB24に保存されている指紋情報が変更された場合に、その使用者識別子と指紋削除通知とを計算機23に送信するように構成されている。計算機23は、指紋認証サーバ25から指紋削除を通知された場合に指紋照合装置22に使用者識別子と指紋削除通知を送信するように構成されている。また、指紋照合装置22は、指紋認証サーバ25に登録されている指紋情報が変更された場合に、指紋DB21に保存されている指紋情報を削除するように構成されており、ここでは、計算機23より指紋削除を通知された場合に、前記使用者識別子に対応する指紋情報を指紋DB21から削除するように構成されている。

【0071】次に動作について図2、図5を用いて説明する。まず、指紋照合装置22は、計算機23の指示により使用者から指紋情報の採取を行う(ステップS31)。この時に、指紋情報を採取する使用者の使用者識別子も計算機23より受取る。そして、上記の使用者識別子を用いて指紋DB21にアクセスして該当使用者の指紋情報が保存されているかを判断する(ステップS32)。指紋情報が保存されていない場合は、計算機23にその採取した指紋情報を送信する(ステップS34)。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する(ステップS33)。ステップS33で、指紋照合が一致した場合には、採取した指紋情報を計算機23に送信する(ステップS34)。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う(ステップS31)。

【0072】次に、計算機23は、受信した指紋情報を使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS35)。

【0073】次に、指紋認証サーバ25は、受信した認証情報と認証DB24に保存されている認証情報を用いて認証を行う(ステップS36)。認証成功の場合には、認証成功的レスポンスを計算機23に送信する。認証失敗の場合には認証失敗のレスポンスを計算機23に送信する。

【0074】次に、計算機23は、指紋認証サーバ25のレスポンスが認証成功の場合、アプリケーションの実行をする(ステップS37)。認証失敗の場合、ユーザに通知して終了する。

【0075】次に、計算機23でアプリケーションが実行された場合(ステップS37)、指紋照合装置22は、指紋DB21に該当指紋情報が保存されているかを判断する(ステップS38)。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋DB21に保存する(ステップS39)。

【0076】次に、認証DB24の指紋情報を変更した場合の動作について図5を用いて説明する。指紋認証サ

バーサスは、認証DB24に保存されている指紋情報が変更されると(ステップS61)、指紋削除通知と該当使用者識別子を計算機23に送信する(ステップS62)。計算機23は、指紋認証サーバ25より指紋削除が通知されると指紋照合装置22に指紋削除通知と該当使用者識別子を送信する(ステップS63)。指紋照合装置22は、計算機23より指紋削除を通知されると、使用者識別子の指紋情報が指紋DB21に保存されているかを検査し(ステップS64)、保存されている場合には、該当情報を削除する(ステップS65)。

【0077】以上のように、この実施の形態6のネットワーク指紋認証システムによれば、認証DBに保存された指紋情報が変更された場合に、指紋DBの内容を削除するようにしたことにより、容易に指紋情報の整合性を保つことができる。

【0078】実施の形態7。以上のように、実施の形態6では、認証DBの指紋が変更されたときに指紋DBの内容を削除するものであったが、次に指紋DBの内容を一定期間で削除する実施の形態を示す。

【0079】実施の形態1と同様に図1は、この発明の実施の形態2の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋照合装置22は、指紋DB21に保存された指紋情報を保存してから所定時間後に削除するように構成されている。

【0080】次に動作について図2と図6を用いて説明する。まず、指紋照合装置22は、計算機23の指示により使用者から指紋情報の採取を行う(ステップS31)。この時に、指紋情報を採取する使用者の使用者識別子も計算機23より受取る。そして、上記の使用者識別子を用いて指紋DB21にアクセスして該当使用者の指紋情報が保存されているかを判断する(ステップS32)。指紋情報が保存されていない場合は、計算機23にその採取した指紋情報を送信する(ステップS34)。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する(ステップS33)。ステップS33で、指紋照合が一致した場合には、採取した指紋情報を計算機23に送信する(ステップS34)。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う(ステップS31)。

【0081】次に、計算機23は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS35)。

【0082】次に、指紋認証サーバ25は、受信した認証情報を認証DB24に保存されている認証情報を用いて認証を行う(ステップS36)。認証成功の場合は、認証成功のレスポンスを計算機23に送信する。認証失敗の場合には認証失敗のレスポンスを計算機23に送信する。

【0083】次に、計算機23は、指紋認証サーバ25

のレスポンスが認証成功の場合、アプリケーションの実行をする(ステップS37)。認証失敗の場合、ユーザに通知して終了する。

【0084】次に、計算機23でアプリケーションが実行された場合(ステップS37)、指紋照合装置22は、指紋DB21に該当指紋情報が保存されているかを判断する(ステップS38)。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋DB21に保存する(ステップS39)。

【0085】次に、指紋DB21の指紋情報を変更した場合の動作について図6を用いて説明する。指紋照合装置22は、指紋DB21に保存されている指紋情報が、保存されてから所定時間以上経過しているかを判断する(ステップS71)。所定時間以上経過していれば、指紋情報を削除する(ステップS72)。この動作を所定時間間隔で実行する。

【0086】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋DBの内容を所定時間間隔で調べて、保存してから所定時間経った古い情報を自動的に削除するようにしたことにより、認証DBで指紋情報が変更された場合にも所定時間経過すれば対応できるようになる。また、指紋DBに保存される情報がある程度最新の情報になるとにより、指紋の情報の時間的変化に対応でき、既存の指紋認証サーバ側を変更する必要がなく、端末側(本実施の形態では計算機、指紋照合装置、指紋DB)だけの変更で適用可能である。

【0087】実施の形態8。以上のように、実施の形態7では、指紋DBの内容を所定時間後に削除するものであったが、次に、指紋認証サーバと計算機の間に、前回認証成功した送信指紋情報を使用して送られた指紋情報が正しいものであるかを検査する指紋認証キャッシュ・サーバを設置する実施の形態を示す。

【0088】図10はこの発明の実施の形態8の全体的な構成を示すシステム構成図である。図において、31-1~3は、採取した指紋情報を出力する指紋照合装置である。32-1~3は、前記指紋照合装置31-1~3から出力された指紋情報とその使用者識別子とを含む認証情報を指紋認証キャッシュ・サーバに送信して認証依頼する計算機である。ここでは、指紋取得のための使用者への指示を行うと共に、指紋認証サーバの指紋認証結果に基づいてアプリケーションの制御を行うように構成されている。33-1~3は、使用者識別子と指紋情報とが保存可能な指紋DBである。なお、ここでは、予め使用者識別子と指紋情報とが保存されている。

【0089】34-1~3は、前記計算機32-1~3から送信された認証情報に含まれた指紋情報とその使用者識別子とを前記指紋DB33-1~3と照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DB33-1~3に保存されていない

場合に、前記認証情報を出力する指紋認証キャッシュ・サーバである。また、照合結果が一致しない場合に指紋認証結果として認証失敗を前記計算機32-1～3に送信するように構成されている。なおここでは、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋DB33-1～3に保存されていない場合に、前記使用者識別子と指紋情報を前記指紋DB33-1～3に保存するように構成されている。

【0090】35は、予め登録された使用者識別子と指紋情報を含む認証情報を保存された認証DBである。ここでは、認証の対象となる使用者の使用者識別子や指紋情報を前記アプリケーションに対するアクセス制御情報等を管理するように構成されている。36は、前記指紋認証キャッシュ・サーバ34-1～3から出力された認証情報を上記認証DB36と照合し、その指紋認証結果を前記指紋認証キャッシュ・サーバ34-1～3に送信する指紋認証サーバである。37は、前記計算機32-1～3と指紋認証キャッシュ・サーバ34-1～3とを接続するネットワークである。

【0091】次に動作について図8を用いて説明する。まず、指紋照合装置31は、計算機32の指示により使用者から指紋の採取を行い(ステップS81)、採取した指紋情報を計算機32に送信する(ステップS82)。

【0092】次に、計算機32は、受信した指紋情報を使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ25に送信する(ステップS83)。

【0093】次に、指紋認証キャッシュ・サーバ34は、受信した使用者識別子を用いて指紋DB33にアクセスして該当使用者の指紋情報を指紋DB33に保存されているかを判断する(ステップS84)。指紋情報が保存されている場合には、その指紋情報を受信した指紋情報を照合し(ステップS85)、照合が一致した場合には、指紋認証サーバ36に認証情報を送信する(ステップS86)。照合が一致しない場合には、計算機にその結果を通知して終了する。ステップS84で、指紋情報が指紋DB33に保存されていない場合には、そのまま認証情報を指紋認証サーバ34に送信する(ステップS86)。

【0094】次に、指紋認証サーバ34は、受信した認証情報を認証DB35に保存されている情報を用いて認証を行う(ステップS86)。認証成功の場合には、指紋認証キャッシュ・サーバ34経由で計算機32に認証成功のレスポンスを送信する。認証失敗の場合には認証失敗のレスポンスを指紋認証キャッシュ・サーバ34経由で計算機32に送信する。

【0095】次に、計算機32は、指紋認証サーバ36のレスポンスに基づいて認証成功か認証失敗かを判断し(ステップS87)、認証成功の場合は、アプリケーションの実行をする(ステップS88)。認証失敗の場合は、ユーザに通知して終了する。

【0096】次に、計算機でアプリケーションが実行された(ステップS88)場合、すなわち、ステップS86の認証が認証成功の場合に、指紋認証キャッシュ・サーバ34は、指紋DB33に該当指紋情報が保存されているかを判断する(ステップS89)。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報を指紋DB33に保存する(ステップS90)。

【0097】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋認証キャッシュ・サーバで照合を行い、その指紋照合結果が一致した場合、又は、使用者識別子が指紋DBに保存されていない場合に、指紋認証サーバで指紋認証を行うようにしたことにより、指紋認証が認証失敗になると予めわかっている場合には、指紋情報が指紋認証サーバに送信されないので、指紋認証サーバへの送信回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、認証DBで認証情報を一元管理することにより、管理コスト、認証情報の秘匿のセキュリティの向上が可能となる。また、既存のシステムは変更する必要がなく、指紋認証キャッシュ・サーバと指紋DBを計算機と指紋認証サーバとの間に設置するだけで適用可能である。

【0098】また、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋DBに保存されていない場合に、使用者識別子と採取された指紋情報を前記指紋DBに保存するようにしたことにより、次回以降の指紋照合において、当該使用者の指紋照合を指紋認証キャッシュ・サーバで行うことができる、指紋認証サーバの負荷軽減を実現することができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側だけの変更で適用可能である。

【0099】また、指紋認証キャッシュ・サーバで照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたことにより、指紋照合が失敗するものは指紋認証サーバに送信されないので、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。

【0100】また、計算機は、指紋認証サーバ又は指紋認証キャッシュ・サーバでの指紋認証結果に基づいてアプリケーションの制御を行うようにしたことにより、使用者に指紋認証結果に応じたアプリケーションを提供することができる。

【0101】

【発明の効果】以上のように、この発明のネットワーク指紋認証システムによれば、使用者識別子と指紋情報とが保存可能な指紋DBと、入力された使用者識別子と採取した指紋情報を前記指紋DBと照合し、その照合結果

果が一致した場合、又は、前記入力された使用者識別子が前記指紋DBに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、予め登録された使用者識別子と指紋情報を含む認証情報が保存された認証DBと、前記計算機から送信された認証情報と前記認証DBと照合して指紋認証を行う指紋認証サーバとを備えたことにより、認証情報を一元管理できるうえ、指紋認証サーバには指紋照合が成功する可能性が高いものだけが送信されるので、認証失敗による再認証の回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。また、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。また、最終的には指紋認証サーバが指紋認証の判断を行うので、認証精度の整合性を保つことができる。

【0102】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋DBに保存されていない場合に、前記入力された使用者識別子と採取した指紋情報を前記指紋DBに保存するように構成されたことにより、次回以降の指紋照合において、当該使用者の指紋照合を指紋照合装置で行うことができるので、指紋認証サーバの負荷軽減を実現することができるという効果がある。

【0103】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置での指紋照合のしきい値が、指紋認証サーバでの指紋照合のしきい値より低く設定されたことにより、指紋照合認証サーバでの指紋照合で一致するはずの指紋情報が、指紋照合装置での指紋照合で失敗する可能性が低くなるので、より一層の認証失敗による再認証の回数を軽減を実現できるという効果がある。さらに、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【0104】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証成功である度に、当該採取した指紋情報を前記指紋DBに保存するように構成されたことにより、指紋DBに保存された指紋情報は最新のものとなり、指紋照合装置での照合で失敗する可能性が低くなるので、使用者の指紋の採取の回数が少なくなり、使用者の利便性の向上が実現できるという効果がある。さらに、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【0105】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証失敗であった場合に当該採取した指紋情報と入力された使用者識別子とを前記指紋DBに保存し、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報と後に採取した指紋情報を照合し、一致する場合には当該後に採取した指紋情報を前記計算機に出力しないように構成されたことにより、以前認証失敗となった指紋情報と同じような指紋情報は指紋認証サーバへ送信されないので、より一層の認証失敗による再認証の回数を軽減を実現できるという効果がある。さらに、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【0106】また、次の発明のネットワーク指紋認証システムによれば、前記計算機は、前記採取した指紋情報と前記指紋DBに保存された指紋情報との照合度を使用者に提示可能に構成されたことにより、使用者の指置きの学習による指紋情報の安定化が期待でき、より一層の認証失敗による再認証の回数を軽減を実現できるという効果がある。また、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【0107】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記指紋認証サーバに登録されている指紋情報が変更された場合に、前記指紋DBに保存されている指紋情報を削除するように構成されたことにより、容易に指紋情報の整合性を保つことができるので、指紋情報の変更されるネットワーク指紋認証システムにおいても、適応可能であるという効果がある。

【0108】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記指紋DBに保存された指紋情報を所定時間後に削除するように構成されたことにより、認証DBで指紋情報が変更された場合にも所定時間経過すれば対応できるようになるという効果がある。また、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【0109】さらにまた、次の発明のネットワーク指紋認証システムによれば、採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、使用者識別子と指紋情報を含む可能な指紋DBと、前記計算機から送信された認証情報に含まれた指紋情報とその使用者識別子とを前記指紋DBと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋DBに保存されていな

い場合に、前記認証情報を出力する指紋認証キャッシュ・サーバと、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証DBと、前記指紋認証キャッシュ・サーバから出力された認証情報と上記認証DBと照合して指紋認証を行う指紋認証サーバとを備えたことにより、認証情報を一元管理できるうえ、指紋認証サーバには指紋照合が成功する可能性が高いものだけが送信されるので、認証失敗による再認証の回数を軽減でき、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。また、既存のネットワーク指紋認証システムへ適用する場合、既存のシステムの変更は必要なく、指紋認証キャッシュ・サーバと指紋DBを計算機と指紋認証サーバとの間に設置するだけで適用することができる。また、最終的には指紋認証サーバが指紋認証の判断を行うので、認証精度の整合性を保つことができる。

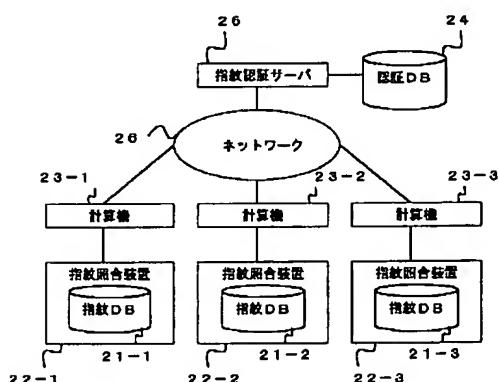
【0110】また、次の発明のネットワーク指紋認証システムによれば、前記指紋認証キャッシュ・サーバは、照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたことにより、指紋照合が失敗するものは指紋認証サーバに送信されないので、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。

【0111】また、次の発明のネットワーク指紋認証システムによれば、前記計算機は、前記指紋認証結果に基づいてアプリケーションの制御を行うように構成されたことにより、使用者に指紋認証結果に応じたアプリケーションを提供することができるという効果がある。

【図面の簡単な説明】

【図1】 実施の形態1～7のシステム構成を示すブロック図である。

【図1】



\* 【図2】 実施の形態1、2、5、6、7の動作を示すフロー図である。

【図3】 実施の形態3の動作を示すフロー図である。

【図4】 実施の形態4の動作を示すフロー図である。

【図5】 実施の形態6の動作を示すフロー図である。

【図6】 実施の形態7の動作を示すフロー図である。

【図7】 実施の形態8のシステム構成を示すブロック図である。

【図8】 実施の形態8の動作を示すフロー図である。

【図9】 従来技術のシステム構成を示すブロック図である。

【図10】 従来技術の動作を示すフロー図である。

【図11】 従来技術の動作を示すフロー図である。

【符号の説明】

11-1～3 コンピュータシステム 12 通信網

13-1～3 データ縮退ユニット 14-1～3

特徴計測ユニット

15-1～3 ファイルシステム 21-1～3

指紋DB

20 22-1～3 指紋照合装置 23-1～3

計算機

24 認証DB 25 指紋認証

サーバ

26 ネットワーク 31-1～3

指紋照合装置

32-1～3 計算機 33-1～3

指紋DB

34-1～3 指紋認証キャッシュ・サーバ 35 認

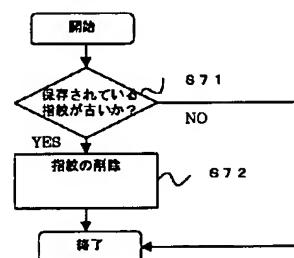
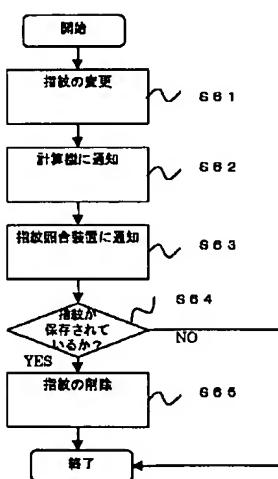
証DB

36 指紋認証サーバ 37 ネ

ットワーク

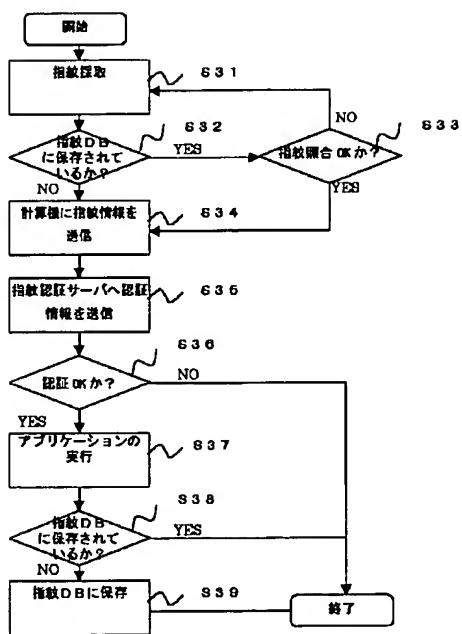
\*

【図5】

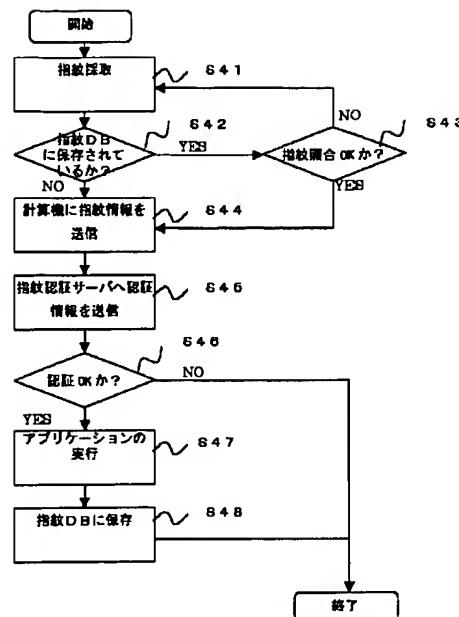


【図6】

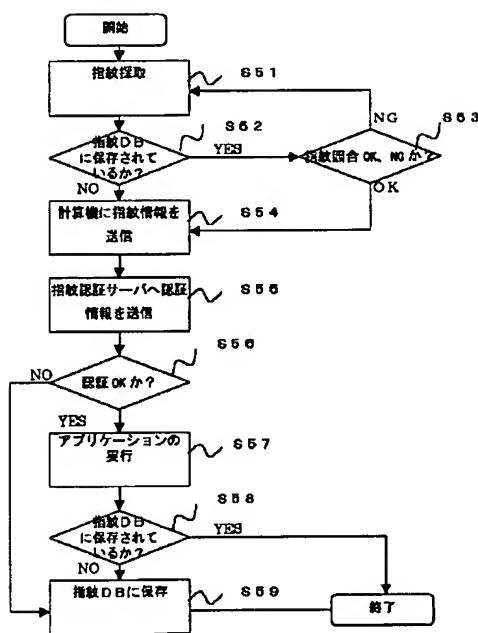
【図2】



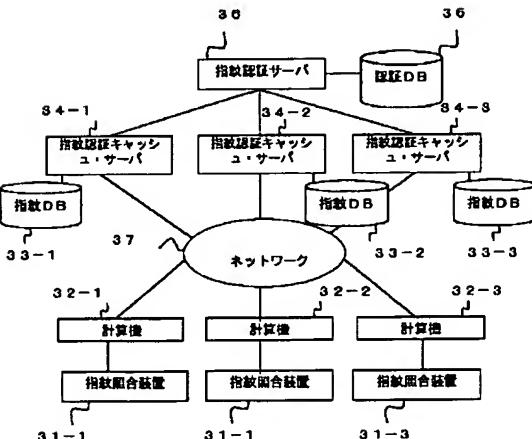
【図3】



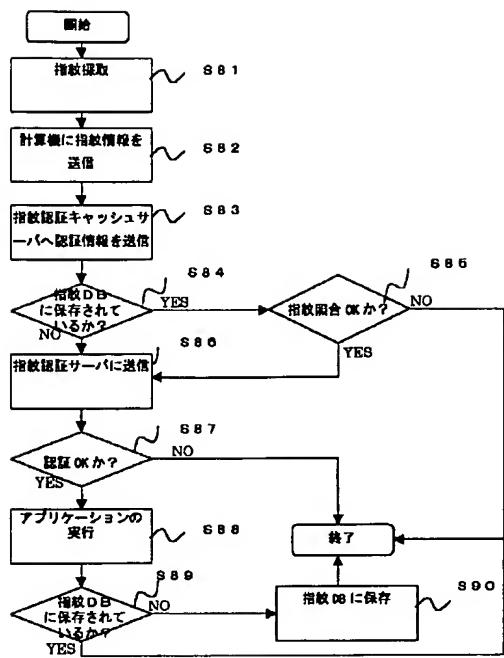
【図4】



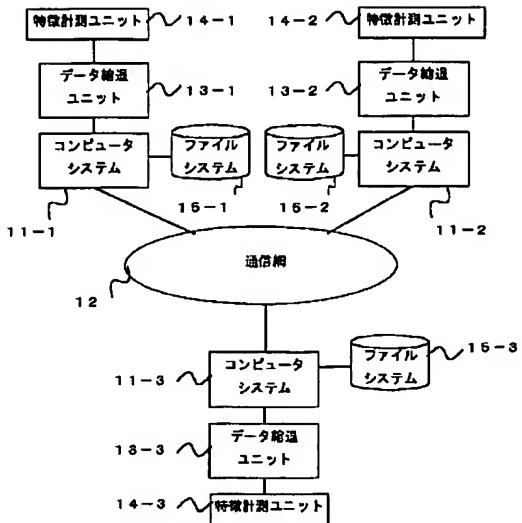
【図7】



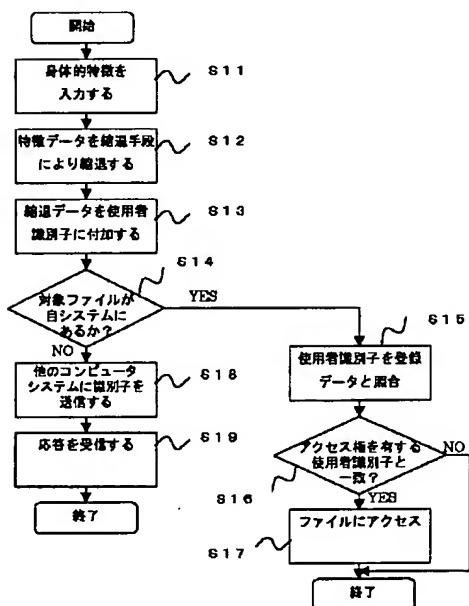
【図8】



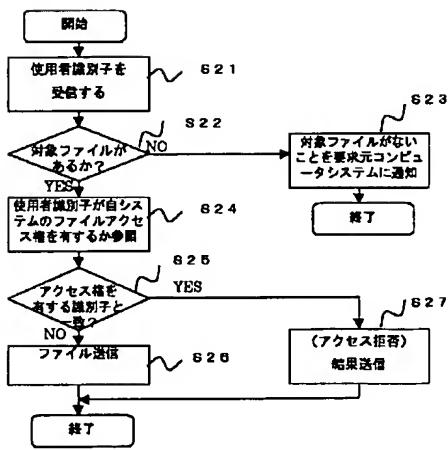
【図9】



【図10】



【図11】



## フロントページの続き

(72)発明者 岡崎 直宣  
東京都千代田区丸の内二丁目2番3号 三  
菱電機株式会社内  
(72)発明者 中村 浩  
東京都千代田区丸の内二丁目2番3号 三  
菱電機株式会社内

(72)発明者 藤井 照子  
東京都千代田区丸の内二丁目2番3号 三  
菱電機株式会社内  
F ターム(参考) SB043 AA09 BA02 CA05 CA09 CA10  
FA02 FA03 FA07 FA08 GA01  
SB085 AE02 AE26 BG07